PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, G08B 13/22, 25/00 — A1

(11) International Publication Number: WO 97/09667

(43) International Publication Date: 13 March 1997 (13.03.97)

(21) International Application Number: PCT/SE96/01103

(22) International Filing Date: 5 September 1996 (05.09.96)

(30) Priority Data:
9503047-4 5 September 1995 (05.09.95) SE

(71)(72) Applicants and Inventors: DANIELSSON, Daniel [SE/SE]; Sjöstorpsvägen 9, S-240 10 Dalby (SE). BJÖRCK, Bertil [SE/SE]; Vitsippevägen 6, S-243 39 Höör (SE).

(74) Agents: STRÖM, Tore et al.; Ström & Gulliksson AB, P.O. Box 4188, S-203 13 Malmö (SE).

(81) Designated States: JP, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

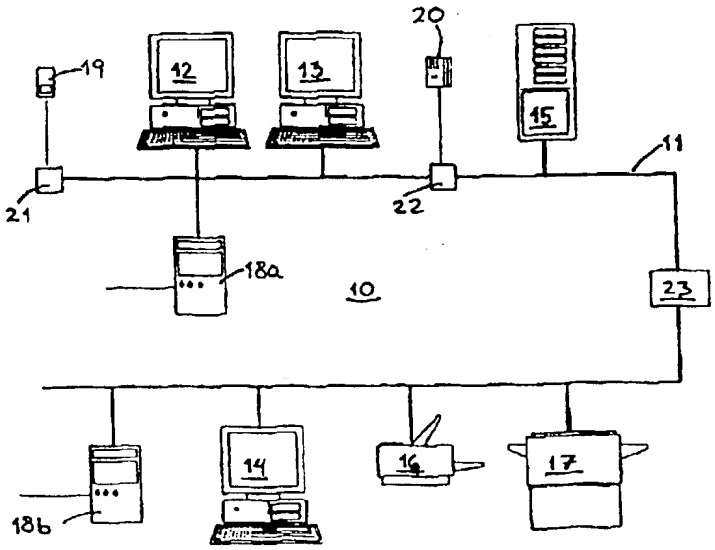
Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

In English translation (filed in Swedish).

(54) Title: METHOD OF MONITORING A COMPUTER SYSTEM



(57) Abstract

A method is provided of monitoring a computer system (10), comprising a plurality of client computers (12, 13, 14), at least one server computer (15) and a wirebased or wireless network (11), by means of which each unit in the system is operatively connected to at least one other unit in the system. In at least some of the client computers information is continuously collected about each respective client computer. The client computer information collected is supplied to an alarm unit comprised in the computer system with the network acting as information carrier and in accordance with the same network protocol(s), which is/are normally used in the computer system (10). In the alarm unit the client computer information received is compared with previously received client computer information, and by means of the alarm unit an alarm signal is generated, if the difference between the client computer information received and the previously received client computer information is larger than a predetermined amount of information.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic			SE	Sweden
CG	Congo	KR	Republic of Korea	SG	Singapore
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LR	Liberia	SZ	Swaziland
CS	Czechoslovakia	LT	Lithuania	TD	Chad
CZ	Czech Republic	LU	Luxembourg	TG	Togo
DE	Germany	LV	Latvia	TJ	Tajikistan
DK	Denmark	MC	Monaco	TT	Trinidad and Tobago
EE	Estonia	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	UG	Uganda
FI	Finland	ML	Mali	US	United States of America
FR	France	MN	Mongolia	UZ	Uzbekistan
GA	Gabon	MR	Mauritania	VN	Viet Nam

METHOD OF MONITORING A COMPUTER SYSTEM

Technical field

The present invention relates to a method of monitoring a computer system, comprising a plurality of client computers, at least one server computer, and a wire-based or wireless network, by means of which every unit in the system is operatively connected to at lest one other unit in the system.

Description of the prior art

Some decades ago the term computer network almost entirely referred to a mainframe or mini computer type of system. Such computer systems were, and still are, in principle based upon a central mainframe or mini computer, which is connected to a plurality of user terminals in a network structure. In such a system the central computer provides all processing power or "intelligence" to the system, while the user terminals are mainly provided as means for user communication, i.e. monitor and keyboard. The central computer handles all software program execution, at the same time controlling peripheral units, such as printers and tape stations, as well as handling external communications, such as telephone-based modem connections. The central computer accepts commands from the users by regularly and sequentially addressing the various terminals, and in response thereof the central computer executes certain pieces of software code and supplies resulting information back to the users. To be able to serve even a large number of connected users without any excessively long response times, such a central mainframe or mini computer comprises high-performance components, which are expensive as well as space demanding.

During the last decade or so another scenario has developed. Thanks to the progress within the field of electronics it has become possible to miniaturise and

integrate computer components, and this has resulted in an almost exponential increase in computer performance, while the relative cost per unit of performance steadily has been reduced. This in turn has made it possible to decentralise the computer processing by providing the user terminals with hardware and software equipment required for execution of computer programs. As a consequence the user terminals may be assigned some of the tasks previously assigned to the central computer, thereby allowing the latter to be made simpler as well as at a lower cost. An additional advantage of such decentralised computer processing is the substantially improved opportunities of user friendly interfaces.

The user terminals referred to above are nowadays usually referred to as client computers, or merely "clients". The most common types of client computers are IBM PC-compatible personal computers, personal computers of the Macintosh-series, or Unix-type workstations. The central computer referred to above today usually corresponds to a so called server computer, or just "server". The task of a server computer is to provide service to a plurality of connected client computers in some way. Common server tasks are storing data and program files of common interest to at least some of the client computers, handling printouts from the client computers, maintaining a sufficient level of data security and integrity within the system by requiring passwords from the users, managing safety backups of data and program files, etc.

In modern computer systems the network is usually physically represented by a plurality of coaxial or twisted pair electric cables, by means of which the various units in the system are interconnected. The client computers, usually appearing at large numbers and normally belonging to any of the client computer types described above, are

connected to the physical network by means of for instance network cards or communication ports. The client computers may for instance be provided with operating systems such as MS-DOS and/or Windows, OS/2 or Unix. Some client operating systems are able to handle a direct network access. Other systems, such as MS-DOS and Windows, must be provided with additional software modules, such as Novell Netware, for network access. Furthermore, one or several server computers are connected to the network. A server computer is usually realized by some type of powerful micro computer administrating the network by means of any network operating system available on the market, among which Novell Netware, Windows NT, Unix, LAN Manager and AppleTalk are the most common. Even mainframe and mini computers of the kinds described above may be connected to the network and function as server computers through an appropriate software interface.

A very important aspect in network systems is data security. Traditionally a high level of data security is regarded to be fulfilled, if the system in question is provided with carefully selected routines for safety backup copying of data and program files to external storage media (such as magnetic tapes), as well as routines for authorization control when accessing the network (login control with respect to passwords, authority levels with respect to the authorities given to individual users, etc). Recently, a third kind of security problems has emerged, namely theft or attempted theft of computers and peripherals comprised in the network.

As long as the computer systems were traditional mainframe and mini computer systems, respectively, the theft risk was low or even negligible. Certainly, it did happen on rare occasions that unauthorized people accessed the computer centrals and stole parts of the computer equipment, but due to the very low demand for such stolen

and cubic-meter sized central computers, and since the user terminals were substantially useless to third persons, such theft activities were hardly prosperous. Today the situation is completely different. As even our homes are being computerized with normal PC-compatible or Macintosh type personal computers, there is a substantially higher demand for stolen computer equipment. Most client computers are today well-equipped personal computers with monitors, and may in principle be used directly even outside a network.

Furthermore, it has become more and more common that the persons carrying out the burglaries and thefts are provided with expert knowledge on the economic values of the components comprised in the computers. Hence, a burglar of today is often aware of the fact that components such as internal memory circuits, hard disks, CD-ROM players, motherboards, etc, are to be regarded as valuable, since not only may they be easily disassembled and carried away, but they are also attractive on the market of stolen property. Consequently, it is nowadays common that the burglar will not, as before, steal and carry away complete computers, but instead remove the computer housing or the like and to some extent consider the values of the individual components in the computers so as to steal only such components, which are found to be of interest.

It may easily be perceived that the problems above are a threat to data security. Besides the strictly economical cost of replacing stolen computers or computer components, the victim is in addition subjected to the inconvenience, as well as the economical loss inherent thereof, that the attacked computers - and in worse cases the entire system - are useless, until the stolen equipment has been replaced. If the stolen equipment comprises permanent storage means such as hard disks, etc, there is also a risk of having business-sensitive data stored thereon disappearing from the company. Another negative consequence of a

computer theft as described above is the tendency of certain criminal individuals of returning to the crime scene after some time, in order to carry out a new round of burglary, since the stolen equipment will then probably have been replaced by new and even more attractive equipment.

Previously known attempts of preventing theft of computers and peripherals have been directed to installation of a conventional and separately arranged anti-theft system, for instance a surveillance system with infrared or acoustic intruder detection means, sometimes combined with burglary sensors attached to windows and doors. Such a conventional anti-theft system has the disadvantage of requiring an extensive wiring and detector installation. In addition, by experience among criminal individuals methods have been developed of avoiding conventional surveillance equipment, for instance by making a survey of the various detector locations in the premises on beforehand and then only carrying out the burglary in such zones, which are out of reach of the detectors. Furthermore, some alarm systems may be deactivated by interrupting the supply of power to a central unit comprised in the alarm system.

Summary of the invention

According to the invention there is provided a method of monitoring a computer system, comprising a plurality of client computers, at least one server computer, and a wire-based or wireless network, by means of which each unit in the system is operatively connected to at least one other unit in the system. The fundamental idea of the present invention is to make use of the already existing network to continuously check that all computers and peripherals connected to the network are still present in an original state. Should the contact with any of the units in the system be lost, for instance due to an unauthorized removal

of units in the system, or parts of these units, this event will be detected and an alarm signal will be generated in response thereto. As a consequence the monitoring may be more accurately performed as well as at a lower cost than with the conventional surveillance equipment described above, partly thanks to the eliminated need for any new wire installation and thanks to the fact that conventional methods of deactivating such conventional surveillance equipment are no longer applicable.

The object of the invention is achieved by a method of monitoring a computer system with the features appearing from the appended patent claims.

Brief description of the drawing

Preferred applications of the method according to the invention will now be described in more detail in the following, reference being made to the accompanying drawing, on which FIG 1 schematically illustrates an exemplary computer system, in which the method according to the invention is applied.

Description of preferred applications

In FIG 1 there is shown an example of how the invention may be applied in a modern computer system. The computer system 10 of FIG 1 comprises a wire-based network 11, to which a plurality of client stations 12, 13, 14 as well as a server computer 15 are connected. Additionally common types of peripherals, such as printers and modems, may be connected to the network 11. Furthermore, in FIG 1 it is indicated that even other kinds of peripherals, such as telefax and copying machines 16, 17, may be directly connected to the network. There is already today a clear tendency at certain companies to connect such equipment to the network, and it must be regarded as likely, that the

computer networks of the future will comprise a variety of such equipment.

Preferably the network 11 is physically comprised of an electric wiring of coaxial cable or twisted-pair cable type, but also other alternatives are possible; wirebased as well as wireless. Low-level communication is occurring on the network in accordance with any established standard, such as the network protocols Ethernet or Token Ring, both of which are members of the IEEE 802 family. High-level communication is occurring according to a standard suitable for the low-level protocol chosen, for instance Novell SPX/IPX or the Unix's TCP/IP protocol. For accessing the network the connected units are provided with appropriate interface means, such as a network card corresponding to the network protocols chosen. According to the invention each network unit, that is to be monitored, is provided with a surveillance module with the following features.

The surveillance module is capable of continuously monitoring its host unit, i.e. the computer, printer, copying machine, etc, to which the surveillance module belongs, so as to detect any change in configuration or other status. The surveillance module may for instance be arranged to detect when the housing of the host unit is opened, when components comprised in the host unit are removed, when the supply of power to the host unit is interrupted, or whenever the host unit loses contact with the network.

According to another preferred application the surveillance module may instead be arranged to collect status information about the host unit at given moments in time, i.e. with no particular focus on a change in status.

Furthermore, the surveillance module is arranged to supply the detected or collected information described above through the network 11 to an alarm unit comprised in the computer system. Preferably, this communication occurs

according to any network protocol already used in the computer system, thereby avoiding conflicts with other hardware and software within the system.

The simplest way of realizing the surveillance module is to provide the existing network card with a sensor, which is arranged to detect whenever the host unit is opened. It is of greatest importance that the surveillance module - in this case the sensor - is operational, even when the rest of the host unit is powerless, for instance due to a deliberate interruption of the power supply in connection with an attempted burglary. Hence, the surveillance module is preferably provided with its own power source, for instance a longlife battery. Such batteries are already today used in a variety of applications, and hence they are not described in more detail here.

Whenever the sensor detects that the host unit has been opened or that the ordinary power supply has been interrupted, the sensor will report this condition through the network to the afore-mentioned alarm unit, which will be described further below.

In a more advanced application the surveillance module is arranged to collect information according to the above about the configuration of the host computer, i.e. the number and size of internal memory circuits, the presence of secondary storage such as a hard disk or a CD-ROM player, the presence of a graphic card and a monitor connected to the host unit, etc. According to this application the host computer will be supplemented by certain hardware and/or software, so that the surveillance module may be in a continuous contact with the different parts or components in the host computer. This concept, which may be referred to as "Safety Channel", will hence mean that certain selected components in a host computer will be in constant operative connection with a surveillance module in the host computer. In accordance with the more simple app-

lication described above the "Safety Channel" application will be supplemented by a battery or another type of uninterruptable power source. The surveillance module itself may for instance be realized as an electronic circuit on the network circuit board, as an independent expansion card or as a software module alone, which may be integrated on a low-level basis in the operating system of the host computer or which as an alternative may be executed as a memory resident program module.

The alarm unit referred to above is operatively connected to the network 11 and is adapted to receive information from the surveillance module of each respective monitored network unit. The alarm unit - which may be realized as a software module in the server computer 15, as a software module in any of the client computers 12, 13, 14 comprised in the computer system 10, or as a separate unit connected to the network - will continuously check the incoming information so as to detect an unauthorized manipulation of equipment within the computer system 10, for instance an attempted theft.

In such applications where the surveillance modules according to the above themselves will detect a change in the equipment within their respective host unit, the alarm unit simply has to generate an external alarm signal, whenever any surveillance module has reported such a change. If, however, the surveillance modules are arranged to report the momentary status for the equipment, the alarm unit will be provided with a conventional electronic memory, in which the expected status for each monitored network unit is stored. The expected status may for instance be information about internal memory or hard disk size, the number of peripherals connected, such as CD-ROM player and monitor, etc. Whenever the reported status deviates from the expected status stored in the electronic memory, an external alarm signal will be generated.

Furthermore, the alarm unit may be arranged to regularly and sequentially poll the monitored units itself and command them to supply their respective status information according to the above. Also this polling activity occurs according to the same network protocol, which is normally used in the computer system.

The external alarm signal is preferably an alarm to a security company, the police or the security managers at the company, for instance by having the alarm signal activate a communication program run on any client computer 12, 13, 14 or server computer 15 within the computer system 10, wherein the program will call the desired party by means of a modem. In order to further increase the security separate cellular telephones or radio transmitters 18a, 18b may be connected to the computer system 10, wherein the alarm may take place wirelessly to the receiving cellular telephone or radio receiver.

Even the server computer 15 comprised in the computer system may be provided with a surveillance module according to the above and take part among the monitored units, if the alarm unit is realized as an individual unit separated from the server computer, which in accordance with the surveillance modules described above is provided with an uninterruptable power supply by means of a battery or the like.

According to a more advanced application the alarm unit - be it realized as a software module in a computer or as a separate unit - may be programmed in such a way, that different alarm conditions are used. For instance, an interruption of the normal power supply of the computer system may be allowed without giving an alarm, provided that the interruption is not followed by any reports on other kinds of disturbances, thereby avoiding that a false alarm is given for instance during thunderstorms. In addition the alarm unit may be programmed to supply more

detailed alarm information, when external alarm is given, for instance by reporting the kind of change that has taken place in the computer system, or which pieces of equipment that have been affected.

It is also possible to practice the method of monitoring according to the invention in combination with already existing conventional surveillance equipment, such as intruder detectors 19 or entrance control units 20. Such conventional units are then provided with modified surveillance modules 21, 22, which are arranged to receive an alarm signal from the detectors 19 and the units 20, respectively, and forward these through the network 11 to the alarm unit described above.

Additionally, the network 11 may be galvanically separated by means of network section units 23. Every section of the network 11 is then preferably provided with its own alarm unit, said alarm units being able to monitor each other to cause an alarm, should any other alarm unit or section of the network be made inoperational. Alternatively, the entire network 11, or portions thereof, may consist of a wire-based optical or a wireless communication link, respectively, of previously known design.

The description above for the preferred applications of the method according to the invention are only to be taken as examples. Other applications may deviate from what has been described above within the scope of the invention, as defined in the appended patent claims. In particular, the term server computer is to be interpreted in a broad sense; the server computer 15 may be constituted by a pure printer and application server (a so called network server) in a "real" server network, but alternatively, it may be represented by any given client computer 12, 13, 14 in a "peer-to-peer" network, in which the different client computers mutually share their own resources as well as

printers and hard disks, and consequently act as client computers as well as server computers.

CLAIMS

1. A method of monitoring a computer system (10), comprising a plurality of client computers (12, 13, 14), at least one server computer (15), and a wirebased or wireless network (11), by means of which each unit in the system is operatively connected to at least one other unit in the system, c h a r a c t e r i z e d by the steps of

continuously collecting information about at least some of the client computers (12, 13, 14) in each respective client computer;

supplying the collected client computer information to an alarm unit comprised in the system (10) with the network (11) acting as information carrier and in accordance with the same network protocol(s) that is/are normally used in the computer system (10);

comparing in the alarm unit the client computer information received with previously received client computer information; and

generating an alarm signal by means of the alarm unit, if the difference between the client computer information received and the previously received client computer information is larger than a predetermined amount of information.

2. A method according to claim 1, c h a r a c t e r i z e d in that said client computer information comprises information about the operative connection between the client computer (12, 13, 14) and the rest of the computer system (10).

3. A method according to claim 1, c h a r a c t e r i z e d in that said client computer information comprises information about components in the client computer (12, 13, 14), such as internal memory, hard disk, CD-ROM player, etc.

4. A method according to any preceding claim, c h a r a c t e r i z e d in that said network (11) at least partly is constituted by a set of electrical wires of coaxial cable or twisted-pair cable type.

5. A method according to any preceding claim, c h a r a c t e r i z e d in that said network (11) is at least partly constituted by an optical fibre cable.

6. A method according to any preceding claim, c h a r a c t e r i z e d in that said network protocol(s) is/are in accordance with any of the network standards IEEE 802.3, IEEE 802.4 or IEEE 802.5.

7. A method according to any preceding claim, wherein the computer system (10) further comprises peripheral equipment (16, 17), c h a r a c t e r i z e d by the additional steps of

continuously collecting information also in said peripheral equipment (16, 17) about the equipment itself as well as components comprised therein;

supplying the collected peripheral equipment information to an alarm unit comprised in the computer system with the network acting as information carrier;

comparing peripheral equipment information received in the alarm unit with previously received peripheral equipment information; and

generate an alarm signal by means of the alarm unit, if the difference between the peripheral equipment information received and the previously received peripheral equipment information is larger than a predetermined amount of information.

8. A method according to claim 7, c h a r a c t e r i z e d in that said peripheral equipment (16, 17) at least partly comprises telefax equipment (16).

9. A method according to claim 7, c h a r a c t e r i z e d in that said peripheral equipment (16, 17) at least partly consists of a copying machine (17).

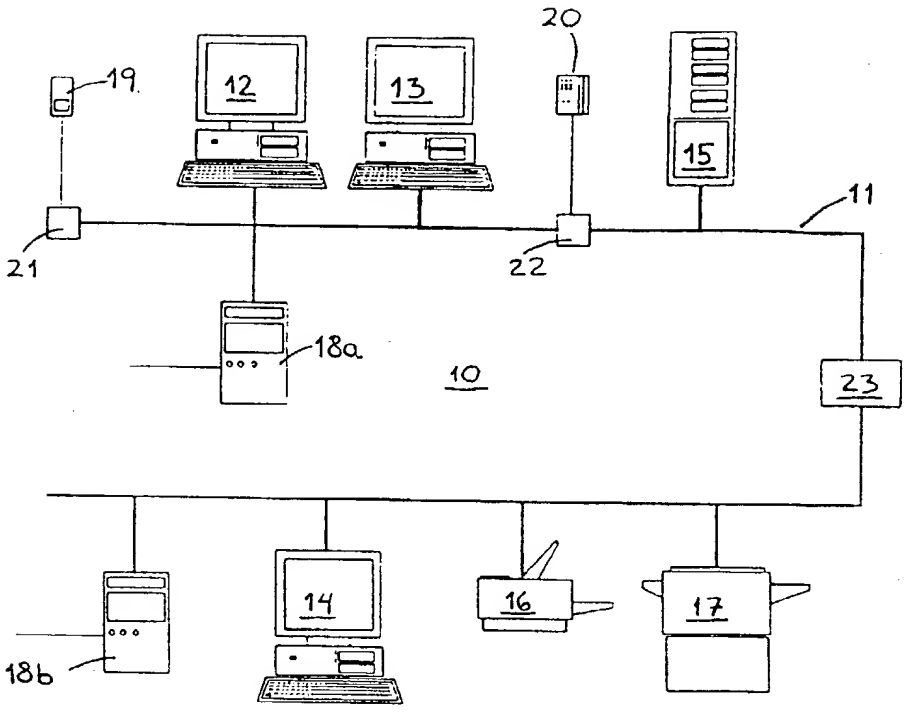
10. A method according to claim 7, c h a r a c t e r i z e d in that said peripheral equipment at least partly is constituted by conventional surveillance equipment (19, 20).

11. A method according to any preceding claim, c h a r a c t e r i z e d in that all monitored units (12, 13, 14; 16, 17) are provided with their own power source, said power source being operational also when the rest of the computer system (10) is powerless.

12. A method according to any preceding claim, c h a r a c t e r i z e d by the additional step of when said alarm signal is generated by the alarm unit, establishing a telephone-based contact with at least one subscriber, who is located outside the premises, in which the computer system (10) is situated.

13. A method according to any preceding claim, c h a r a c t e r i z e d in that the alarm unit is constituted by a computer program executed or run in said server computer (15) or in any of the client computers.

Fig 1



INTERNATIONAL SEARCH REPORT

International application No.
PCT/SE 96/01103

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: G06F 1/00, G08B 13/22, G08B 25/00
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPODOC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5406260 A (MARSHALL B. CUMMINGS ET AL), 11 April 1995 (11.04.95) -- ---	1-13

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 January 1997	16 -01- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Jan Silfverling Telephone No. +46 8 782 25 00

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/10/96

International application No.
PCT/SE 96/01103

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 5406260	11/04/95	NONE	